(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－256113
（P2001－256113A）
(43)公開日　平成13年９月21日(2001.9.21)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ａ　５Ｂ０１７

審査請求　未請求　請求項の数14　ＯＬ　（全 12 頁）

(21)出願番号　特願2000－69262(P2000－69262)

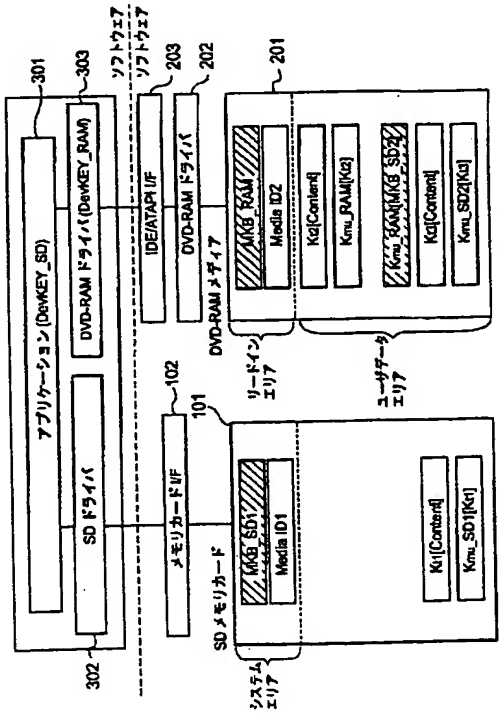
(22)出願日　平成12年３月13日(2000.3.13)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　石橋　泰博
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5B017 AA01 BA02 BA05 BA07 BB02
BB06 CA09 CA14 CA16

(54)【発明の名称】　コンテンツ処理システムおよびコンテンツ保護方法

(57)【要約】
【課題】ある特定のメディア種別に対応したデバイス識別情報によって他のメディア種別の記録メディアを扱う。
【解決手段】ＤＶＤ－ＲＡＭドライバ３０３のインストール時には、ＳＤメモリカード用の最新のメディアキーブロック（ＭＫＢ＿ＳＤ２）がＷＥＢサーバやＤＶＤ－ＲＡＭドライバ３０３用のインストールＣＤなどから取得され、それがＤＶＤ－ＲＡＭメディア２０１のユーザデータエリアに書き込まれる。アプリケーションプログラム３０１からのＤＶＤ－ＲＡＭメディア２０１に対する認証要求があると、ＤＶＤ－ＲＡＭメディア用のメディアキーブロック（ＭＫＢ＿ＲＡＭ）の代わりに、ＳＤメモリカード用の最新のメディアキーブロック（ＭＫＢ＿ＳＤ２）がＤＶＤ－ＲＡＭメディア２０１から読み出され、それがアプリケーションプログラム３０１に渡される。



1

【特許請求の範囲】

【請求項１】　記録メディアに予め記録された、排除すべき電子機器のデバイス識別情報を特定可能なリボケーションリスト情報と、前記記録メディアを扱う電子機器のデバイス識別情報とを用いて、前記記録メディアと電子機器間の認証を行うコンテンツ処理システムであって、

前記デバイス識別情報およびそれに対応する前記リボケーションリスト情報は、記録メディアの種別毎に異なっており、

第１のメディア種別に対応するリボケーションリスト情報に対応した第１のデバイス識別情報を有する電子機器で第２のメディア種別の記録メディアを扱う場合、前記第２のメディア種別の記録メディアに対応した制御プログラムによって、前記第１のメディア種別に対応するリボケーションリスト情報を前記第２のメディア種別の記録メディア上に記録させる手段を具備することを特徴とするコンテンツ処理システム。

【請求項２】　前記第１のデバイス識別情報を有する電子機器上で動作するコンテンツ処理プログラムから前記第２のメディア種別の記録メディアに対する認証要求が発行された場合、前記第２のメディア種別の記録メディアに対応するリボケーションリスト情報に代えて、前記第１のメディア種別に対応するリボケーションリスト情報を前記第２のメディア種別の記録メディアから読み出して前記コンテンツ処理プログラムに渡す手段をさらに具備することを特徴とする請求項１記載のコンテンツ処理システム。

【請求項３】　前記制御プログラムは、前記第２のメディア種別の記録メディアをリード／ライト制御するドライブ装置用のデバイスドライバであることを特徴とする請求項１記載のコンテンツ処理システム。

【請求項４】　前記制御プログラムは、前記第１の第２のメディア種別に対応した第２のデバイス識別情報を有しており、その第２のデバイス識別情報と、前記第２のメディア種別の記録メディア上に予め記録されている第２のメディア種別に対応するリボケーションリスト情報とを用いて、前記第２のメディア種別の記録メディアとの認証を行い、正当なもの同士あることが確認された場合に、前記第１のメディア種別に対応するリボケーションリスト情報を前記第２のメディア種別の記録メディア上に記録することを特徴とする請求項１記載のコンテンツ処理システム。

【請求項５】　前記第１のメディア種別に対応するリボケーションリスト情報は、前記制御プログラムが前記第２のメディア種別の記録メディア上に予め記録されているリボケーションリスト情報との認証によって得た暗号化鍵によって暗号化された状態で、前記第２のメディア種別の記録メディア上に記録されることを特徴とする請求項４記載のコンテンツ処理システム。

2

【請求項６】　コンテンツ保護のために排除すべき電子機器のデバイス識別情報を特定するために記録メディアにあらかじめ記憶されたリボケーションリスト情報と、前記記録メディアを扱う電子機器のデバイス識別情報とを用いて、コンテンツ保護に必要な機能を持つ正当なもの同士であるか否かの認証を行い、その認証によって、コンテンツの暗号化／復号化を管理するための記録メディア固有キーを生成するコンテンツ処理システムであって、

前記デバイス識別情報およびそれに対応する前記リボケーションリスト情報は、記録メディアの種別毎に異なっており、

第１のメディア種別に対応するリボケーションリスト情報に対応した第１のデバイス識別情報を有し、前記第１のメディア種別に属する第１の記録メディアとの間の認証によって得た第１の記録メディア固有キーを用いて、コンテンツの記録または読み出しを行うコンテンツ処理手段と、

前記コンテンツ処理手段によって前記第１のメディア種別とは異なる第２のメディア種別に属する第２の記録メディアを使用する場合、前記第１のメディア種別に対応するリボケーションリスト情報を前記第２の記録メディア上に書き込み、その書き込んだリボケーションリスト情報を前記コンテンツ処理手段からの認証要求に応じて前記コンテンツ処理手段に渡すことにより、前記コンテンツ処理手段と前記第２の記録メディアとの間の認証を実行させる制御手段とを具備することを特徴とするコンテンツ処理システム。

【請求項７】　前記第２の記録メディアには、前記第２のメディア種別に対応するリボケーションリスト情報があらかじめ記録されており、

前記制御手段は、前記第２の記録メディアにあらかじめ記録されているリボケーションリスト情報に対応した第２のデバイス識別情報を有し、前記第２の記録メディアとの間の認証によって得た記録メディア固有キーを用いて、前記第１のメディア種別に対応するリボケーションリスト情報を暗号化した後に前記第２の記録メディア上に書き込むことを特徴とする請求項６記載のコンテンツ処理システム。

【請求項８】　前記制御手段は、前記コンテンツ処理手段からの認証要求に応じて、前記第１のメディア種別に対応する前記暗号化されたリボケーションリスト情報を、前記第２の記録メディアとの間の認証によって得た記録メディア固有キーを用いて復号化した後に前記コンテンツ処理手段に渡すことを特徴とする請求項７記載のコンテンツ処理システム。

【請求項９】　前記制御手段は、前記第１のメディア種別に対応する最新のリボケーションリスト情報を外部から取得し、その取得したリボケーションリスト情報を前記第２の記録メディア上に書き込むことを特徴とする請

求項６または７記載のコンテンツ処理システム。

【請求項１０】　前記制御手段は、前記第２のメディア種別の記憶メディアを扱うための記憶装置の制御を行うドライバプログラムであることを特徴とする請求項６記載コンテンツ処理システム。

【請求項１１】　コンテンツ保護のために排除すべき電子機器のデバイス識別情報を特定するために記録メディアにあらかじめ記憶されたリボケーションリスト情報と、前記記録メディアを扱う電子機器のデバイス識別情報とを用いて、コンテンツ保護に必要な機能を持つ正当なもの同士であるか否かの認証を行い、その認証によって、コンテンツの暗号化／復号化を管理するための記録メディア固有キーを生成するコンテンツ処理システムであって、

前記デバイス識別情報およびそれに対応する前記リボケーションリスト情報は、記録メディアの種別毎に異なっており、

電子機器が有するデバイス識別情報では認証することができない別種別の第１のリボケーションリスト情報が予め記憶された第１の記憶メディアを使用する場合、前記電子機器が有するデバイス識別情報に対応したメディア種別用の第２のリボケーションリスト情報を取得して前記第１の記憶メディアに記憶する手段と、

前記電子機器からの前記第１の記憶メディアに対する認証要求に応じて、前記第１の記憶メディアに書き込んだ前記第２のリボケーションリスト情報を前記電子機器に渡すことにより、前記電子機器と前記第１の記録メディアとの間の認証を実行させる手段とを具備することを特徴とするコンテンツ処理システム。

【請求項１２】　コンテンツ保護のために排除すべき電子機器のデバイス識別情報を特定するために記録メディアにあらかじめ記憶されたリボケーションリスト情報と、前記記録メディアを扱う電子機器のデバイス識別情報とを用いて、コンテンツ保護に必要な機能を持つ正当なもの同士であるか否かの認証を行い、その認証によって、コンテンツの暗号化／復号化を管理するための記録メディア固有キーを生成するコンテンツ保護方法であって、

前記デバイス識別情報およびそれに対応する前記リボケーションリスト情報は、記録メディアの種別毎に異なっており、

電子機器が有するデバイス識別情報では認証することができない別種別の第１のリボケーションリスト情報が予め記憶された第１の記憶メディアを使用する場合、前記電子機器が有するデバイス識別情報に対応したメディア種別用の第２のリボケーションリスト情報を取得して前記第１の記憶メディアに記憶することを特徴とするコンテンツ保護方法。

【請求項１３】　前記電子機器から前記第１の記憶メディアに対する認証要求が発行された場合、前記第１の記憶メディアに書き込んだ前記第２のリボケーションリスト情報を前記電子機器に渡すことにより、前記電子機器と前記第１の記録メディアとの間の認証を実行させることを特徴とする請求項１２記載のコンテンツ保護方法。

【請求項１４】　コンテンツ保護のために排除すべき電子機器のデバイス識別情報を特定するために記録メディアにあらかじめ記憶されたリボケーションリスト情報と、前記記録メディアを扱う電子機器のデバイス識別情報とを用いて、コンテンツ保護に必要な機能を持つ正当なもの同士であるか否かの認証を行い、その認証によって、コンテンツの暗号化／復号化を管理するための記録メディア固有キーを生成するコンテンツ処理システムで使用可能なコンピュータプログラムが記録されたコンピュータ読み取り可能な記録媒体であって、

前記デバイス識別情報およびそれに対応する前記リボケーションリスト情報は、記録メディアの種別毎に異なっており、

前記コンピュータプログラムは、

電子機器が有するデバイス識別情報では認証することができない別種別の第１のリボケーションリスト情報が予め記憶された第１の記憶メディアを使用する場合、前記電子機器が有するデバイス識別情報に対応したメディア種別用の第２のリボケーションリスト情報を取得して前記第１の記憶メディアに記憶するステップと、

前記電子機器からの前記第１の記憶メディアに対する認証要求に応じて、前記第１の記憶メディアに書き込んだ前記第２のリボケーションリスト情報を前記電子機器に渡すことにより、前記電子機器と前記第１の記録メディアとの間の認証を実行させるステップとを具備することを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、画像データや音楽データなどの様々なデジタルコンテンツを扱うことが可能なコンテンツ処理システムおよびコンテンツ保護方法に関する。

【０００２】

【従来の技術】近年、コンピュータ技術の発達に伴い、マルチメディア対応のパーソナルコンピュータ、セットトップボックス、プレイヤー、ゲーム機などの各種電子機器が開発されている。この種の電子機器は、記録メディアに格納された画像データや音楽データなどの様々なデジタルコンテンツを再生できるほか、インターネット等を通じてデジタルコンテンツをダウンロードして使用することもできる。

【０００３】これらデジタルコンテンツは、例えばＭＰＥＧ２、ＭＰ３といったデジタル符号化技術の採用により、品質を落とすことなくコピーしたり、ダウンロードすることができる。このため、最近では、著作権保護の観点から、このようなデジタルコンテンツを不正使用か

ら保護するための技術の必要性が叫ばれている。

【０００４】

【発明が解決しようとする課題】そこで、最近では、メモリカードなどのリムーバブルメディアを中心に、正当な著作権保護機能を有する電子機器と記録メディアとの間でのみコンテンツの受け渡しを可能にするための認証および暗号化の仕組みが開発され始めている。

【０００５】代表的な認証および暗号化技術としては、電子機器固有のデバイス識別情報と、記録メディア側に記録されるリボケーションリスト情報と称されるキーマトリクスとを用いて認証を行うことによって、不当な電子機器の排除と正当な電子機器に対する暗号化鍵の発行を行う仕組みが考えられている。この仕組みを用いることにより、出荷時に記録メディアに記録するリボケーションリスト情報のみを最新のものに更新することだけで、ハッキングされたことが発覚したデバイス識別情報についてはその使用を無効化できるようになり、不正な攻撃からコンテンツを保護すること可能となる。

【０００６】リボケーションリスト情報は、そのデータサイズが大きいほど、排除可能なデバイス識別情報の組み合わせを増やすことができることから、できるだけ大きなデータサイズに設定することが好ましい。

【０００７】しかし、実際には、記録メディアの種別毎に記憶容量は大幅に異なるので、異なるメディア種間で共通サイズのリボケーションリスト情報を用いると、種々の弊害が生じることになる。たとえば、メモリカードのように記憶容量が比較的小さい記録メディアについては、リボケーションリスト情報を大きく設定しすぎると、ユーザデータエリアとして割り当てるべきメモリサイズが圧迫されてしまうことになる。また、リボケーションリスト情報によって認証可能なデバイス識別情報の数は有限であるため、メディア種間で共通のリボケーションリスト情報を規定すると、割り当て可能なデバイス識別情報の数の不足等の事態を招くことになる。

【０００８】一方、記録メディアの種別毎に個々にリボケーション情報およびそれに対応するデバイス識別情報を規定すれば、各記録メディア種別に最適なサイズのリボケーションリスト情報を使用することが可能となる。ところが、このようにすると今度は、パーソナルコンピュータなどのように種別の異なる様々な記録メディアを扱うことが可能な機器においては、記録メディア間の互換性に関して以下のような問題が生じることになる。

【０００９】例えば、メモリカード用のデバイス識別情報が割り当てられている正当な機器上で動作するアプリケーションプログラムは、その機器のデバイス識別情報と使用するメモリカード上に予め記録されているリボケーションリスト情報とを用いて認証を行うことにより、そのメモリカード上のコンテンツを扱うことができる。しかし、メモリカード以外の記録メディア、例えばＤＶＤ－ＲＡＭメディアなどを扱う場合には、そのＤＶＤ－ＲＡＭメディア上に予め記録されているリボケーションリスト情報はメモリカード用のデバイス識別情報では扱うことができないため、メモリカードからＤＶＤ－ＲＡＭメディアにコンテンツを移すなどの処理を行うことはできなくなる。よって、ユーザは、著作権保護機能に対応した正当なＤＶＤ－ＲＡＭドライブを新たに購入したとしても、実際にはＤＶＤ－ＲＡＭメディアをメモリカードと同様に扱うことはできない。これは、ユーザにとっては非常に不便なことである。

【００１０】本発明は上述の事情に鑑みてなされたものであり、ある特定のメディア種別に対応したデバイス識別情報によって他のメディア種別の記録メディアを扱えるようにすると共に、さらに、著作権保護機能に対応した正当な記録メディアであればその種別を意識することなく、それら記録メディアを透過的に扱うこともできるコンテンツ処理システムおよびコンテンツ保護方法を提供することを目的とする。

【００１１】

【課題を解決するための手段】上述の課題を解決するため、本発明は、記録メディアに予め記録された、排除すべき電子機器のデバイス識別情報を特定可能なリボケーションリスト情報と、記記録メディアを扱う電子機器のデバイス識別情報とを用いて、記録メディアと電子機器間の認証を行うコンテンツ処理システムであって、前記デバイス識別情報およびそれに対応する前記リボケーションリスト情報は、記録メディアの種別毎に異なっており、第１のメディア種別に対応するリボケーションリスト情報に対応した第１のデバイス識別情報を有する電子機器で第２のメディア種別の記録メディアを扱う場合、前記第２のメディア種別の記録メディアに対応した制御プログラムによって、前記第１のメディア種別に対応するリボケーションリスト情報を前記第２のメディア種別の記録メディア上に記録させる手段を具備することを特徴とする。

【００１２】このように、第２のメディア種別の記録メディアに対応した制御プログラムによって第１のメディア種別に対応するリボケーションリスト情報を第２のメディア種別の記録メディア上に記録することにより、その記録したリボケーションリスト情報を用いて第２のメディア種別の記録メディアとの認証を実行させることが可能となるので、第１のメディア種別に対応したデバイス識別情報で、第２のメディア種別の記録メディアを扱うことができる。よって、著作権保護機能に対応した正当な記録メディアであればその種別を意識することなく、それら記録メディアを扱うことが可能となる。

【００１３】この場合、前記第１のデバイス識別情報を有する電子機器上で動作するコンテンツ処理プログラムから前記第２のメディア種別の記録メディアに対する認証要求が発行された場合、前記第２のメディア種別の記録メディアに対応するリボケーションリスト情報に代え

て、前記第１のメディア種別に対応するリポケーションリスト情報を前記第２のメディア種別の記録メディアから読み出して前記コンテンツ処理プログラムに渡す手段を設けることにより、コンテンツ処理プログラムは、メディア種別の違いを全く意識することなく、第１及び第２のメディア種別を透過的に扱うことが可能となる。

【００１４】また、前記制御プログラムとしては、前記第２のメディア種別の記録メディアをリード／ライト制御するドライブ装置用のデバイスドライバを使用することが好ましい。これにより、ユーザがそのドライブ装置を新たに購入して使用する場合でも、既存の他の記録メディアとの互換性を維持することが可能となり、既存の他の記録メディアに対応するコンテンツ処理プログラムによって異なる種別の記録メディアを透過的に扱うことが可能となる。

【００１５】また、前記制御プログラムは、前記第１の第２のメディア種別に対応した第２のデバイス識別情報を有しており、その第２のデバイス識別情報と、前記第２のメディア種別の記録メディア上に予め記録されている第２のメディア種別に対応するリポケーションリスト情報とを用いて、前記第２のメディア種別の記録メディアとの認証を行い、正当なもの同士あることが確認された場合に、前記第１のメディア種別に対応するリポケーションリスト情報を前記第２のメディア種別の記録メディア上に記録することを特徴とする。これにより、第１のデバイス識別情報のみの機器であっても、内部的に第２のメディア種別の記録メディアとの認証を行うことができるので、コンテンツをより安全に管理することが可能となる。

【００１６】また、前記第１のメディア種別に対応するリポケーションリスト情報は、前記制御プログラムが前記第２のメディア種別の記録メディア上に予め記録されているリポケーションリスト情報との認証によって得た暗号化鍵によって暗号化した状態で、前記第２のメディア種別の記録メディア上に記録することが好ましい。これにより、前記第１のメディア種別に対応するリポケーションリスト情報を第２のメディア種別の記録メディアのユーザデータエリアに書き込んだ場合でも、その秘匿化を実現できる。

【００１７】また、本発明は、コンテンツ保護のために排除すべき電子機器のデバイス識別情報を特定するために記録メディアにあらかじめ記憶されたリポケーションリスト情報と、前記記録メディアを扱う電子機器のデバイス識別情報とを用いて、コンテンツ保護に必要な機能を持つ正当なもの同士であるか否かの認証を行い、その認証によって、コンテンツの暗号化／復号化を管理するための記録メディア固有キーを生成するコンテンツ処理システムであって、前記デバイス識別情報およびそれに対応する前記リポケーションリスト情報は、記録メディアの種別毎に異なっており、第１のメディア種別に対応するリポケーションリスト情報に対応した第１のデバイス識別情報を有し、前記第１のメディア種別に属する第１の記録メディアとの間の認証によって得た第１の記録メディア固有キーを用いて、コンテンツの記録または読み出しを行うコンテンツ処理手段と、前記コンテンツ処理手段によって前記第１のメディア種別とは異なる第２のメディア種別に属する第２の記録メディアを使用する場合、前記第１のメディア種別に対応するリポケーションリスト情報を前記第２の記録メディア上に書き込み、その書き込んだリポケーションリスト情報を前記コンテンツ処理手段からの認証要求に応じて前記コンテンツ処理手段に渡すことにより、前記コンテンツ処理手段と前記第２の記録メディアとの間の認証を実行させる制御手段とを具備することを特徴とする。

【００１８】この構成においても、第１のメディア種別に対応したデバイス識別情報で、第２のメディア種別の記録メディアを扱うことが可能となるので、種別の異なる記録メディアを透過的に扱うことが可能となる。また、コンテンツの暗号化鍵としてメディア固有キーを用いているので、記録メディア単体で他の機器に移動して使用しても、移動先の機器が正当な機器であればコンテンツを再生することができる。

【００１９】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を説明する。

【００２０】図１には、本発明の一実施形態に係るコンテンツ処理システムのシステム構成が示されている。このコンテンツ処理システムは画像データや音楽データなどの各種デジタルコンテンツを扱うためのものであり、たとえばパーソナルコンピュータ（ＰＣ）などの電子機器から構成されている。このコンテンツ処理システムにおけるコンテンツ保護の方法は、コンテンツを記録すべき記録メディア毎にその記録メディア固有のメディア固有キーを用いてコンテンツの暗号化／復号化を管理することを前提としている。これは、同一記録メディアであれば、その記録メディアを他のパーソナルコンピュータや電子機器で使用しても再生できるようにするためであり、コンテンツは各記録メディア毎にそのメディアとの認証によって個々に得られるメディア固有キーを用いて暗号化して記録される。

【００２１】メディア固有キーを用いたコンテンツの暗号化／復号化の管理は、そのための専用機能を内蔵したコンテンツ処理用のアプリケーションプログラム３０１によって実行される。このアプリケーションプログラム３０１は、タンパ・レジスタント・ソフトウェアとして実現されている。タンパ・レジスタント・ソフトウェアとは、不正な内部解析や改竄などの攻撃に対して防衛機能を備えるソフトウェアを意味する。

【００２２】本実施形態においては、コンテンツの記録・読み出しに使用される記録メディアとして、ＳＤ（Se

cure Digital）メモリカード１０１と、ＤＶＤ－ＲＡＭメディア２０１が用いられる。ＳＤ（Secure Digital）メモリカード１０１のリード／ライトは、本電子機器に設けられたメモリカードインターフェース１０２と、ＳＤカード制御用のデバイスドライバプログラムであるＳＤドライバ３０２を介して行われる。また、ＤＶＤ－ＲＡＭメディア２０１のリード／ライトは、本電子機器に設けられたＩＤＥ／ＡＴＡＰＩインターフェース２０３に接続されるＤＶＤ－ＲＡＭドライブ２０２と、その制御用のデバイスドライバプログラムであるＤＶＤ－ＲＡＭドライバ３０３を介して行われる。

【００２３】ＳＤドライバ３０２およびＤＶＤ－ＲＡＭドライバ３０３もタンバ・レジスタント・ソフトウェアとして実現されている。

【００２４】本実施形態では、これら記録メディアを用いたコンテンツの暗号化／復号化管理は、各記録メディアに予め記録されているリボケーションリスト情報と、電子機器毎に予め用意されるその電子機器固有のデバイス識別情報とを用いて行われる。

【００２５】ここで、リボケーションリスト情報とは、コンテンツ保護のために排除すべき電子機器のデバイス識別情報の一覧が埋め込まれた認証用情報であり、認証相手となる電子機器のデバイス識別情報が無効化すべきものであるか否かの判定に使用されると共に、正当なデバイス識別情報であると判定された場合にはメディア固有キーの生成のために用いられる。このリボケーションリスト情報は多数のキーマトリクス情報から構成されおり、以下ではメディアキーブロック（ＭＫＢ）と称することにする。正当な著作権保護機能を有すると認められた記録メディアは、メディアキーブロック（ＭＫＢ）が記録された状態で出荷される。

【００２６】デバイス識別情報は各電子機器毎に割り当てられる固有の識別情報であり、正当な著作権保護機能を有すると認められた電子機器にのみ発行される。各電子機器はデバイス識別情報が埋め込まれた状態で出荷される。以下では、デバイス識別情報をデバイスキー（Ｄｅｖ　ＫＥＹ）と称することにする。

【００２７】メディアキーブロック（ＭＫＢ）の内容は記録メディアの種別毎に異なっており、ＳＤ（Secure Digital）メモリカード１０１とＤＶＤ－ＲＡＭメディア２０１とでは異なるメディアキーブロック（ＭＫＢ）が用いられる。すなわち、ＳＤメモリカード１０１には、ＳＤメモリカード用に規定されたメディアキーブロック（ＭＫＢ＿ＳＤ１）が予め記録されており、またＤＶＤ－ＲＡＭメディア２０１には、ＤＶＤ－ＲＡＭメディア用に規定されたメディアキーブロック（ＭＫＢ＿ＲＡＭ）が予め記録されている。これらメディアキーブロックはそれぞれライトプロテクトされた読み出し専用領域、すなわちＳＤメモリカード１０１についてはシステムエリア、ＤＶＤ－ＲＡＭメディア２０１についてはリードインエリアに記録されている。

【００２８】本実施形態の電子機器に割り当てられているデバイスキー（Ｄｅｖ　ＫＥＹ＿ＳＤ）はＳＤメモリカード用のメディアキーブロックに対応するものであり、アプリケーションプログラム３０１はそのデバイスキー（Ｄｅｖ　ＫＥＹ＿ＳＤ）を用いてＳＤメモリカード１０１との認証を行う。この認証によって正当なもの同士であることが認識されると、アプリケーションプログラム３０１は、認証結果により得られるメディアキーとＳＤメモリカード１０１固有の識別情報であるメディアＩＤ（Ｍｅｄｉａ　ＩＤ１）とを用いて、ＳＤメモリカード１０１に固有の暗号化鍵であるメディア固有キー（Ｋｍｕ＿ＳＤ１）を生成する。ＳＤメモリカード１０１に記録するコンテンツの暗号化およびその復号化の管理は、メディア固有キー（Ｋｍｕ＿ＳＤ１）を用いて行われる。すなわち、アプリケーションプログラム３０１は、ＳＤメモリカード１０１に以下のデータを書き込む。

【００２９】・Ｋｔ１［Ｃｏｎｔｅｎｔ］：　タイトルキーＫｔ１と称される秘密鍵によって暗号化されたコンテンツ

・Ｋｍｕ＿ＳＤ１［Ｋｔ１］：　ＳＤメモリカード１０１のメディア固有キー（Ｋｍｕ＿ＳＤ１）によって暗号化されたタイトルキー

なお、タイトルキーＫｔ１としては例えば乱数などを用いた時変キーを利用することができる。

【００３０】ＤＶＤ－ＲＡＭドライバ３０３は、ＤＶＤ－ＲＡＭメディアをＳＤメモリカードと同様に扱うための機能をアプリケーションプログラム３０１に対して提供する。アプリケーションプログラム３０１とＤＶＤ－ＲＡＭメディア２０１との認証、およびアプリケーションプログラム３０１によるＤＶＤ－ＲＡＭメディア２０１のリード／ライトは、すべてＤＶＤ－ＲＡＭドライバ３０３を介して行われる。

【００３１】ＤＶＤ－ＲＡＭドライバ３０３は、ＤＶＤ－ＲＡＭメディア用のメディアキーブロック（ＭＫＢ＿ＲＡＭ）に対応したデバイスキー（Ｄｅｖ　ＫＥＹ＿ＲＡＭ）を有しており、ＤＶＤ－ＲＡＭメディア２０１との間の認証を行うことができる。さらに、ＤＶＤ－ＲＡＭドライバ３０３には、以下の機能が含まれている。

【００３２】・ＳＤメモリカード用の最新のメディアキーブロック（ＭＫＢ＿ＳＤ２）をＷＥＢサーバやＤＶＤ－ＲＡＭドライバ３０３用のインストールＣＤなどから取得し、それをＤＶＤ－ＲＡＭメディア２０１のユーザデータエリアに書き込む機能

・アプリケーションプログラム３０１からのＤＶＤ－ＲＡＭメディア２０１に対する認証要求に応答して、ＤＶＤ－ＲＡＭメディア用のメディアキーブロック（ＭＫＢ＿ＲＡＭ）の代わりに、ＳＤメモリカード用の最新のメディアキーブロック（ＭＫＢ＿ＳＤ２）をＤＶＤ－ＲＡ

Mメディア２０１から読み出して、アプリケーションプログラム３０１に渡す機能
これら機能の詳細は図４以降で詳述する。

【００３３】（メディアキーブロック）次に、図２を参照して、メディアキーブロックとデバイスキーとの関係を説明する。前述したように、メディアキーブロックとデバイスキーは記録メディアの種別毎に個々に規定される。図２（Ａ）はＳＤメモリカード用のメディアキーブロック（ＭＫＢ＿ＳＤ１）とデバイスキー（ＤｅｖＫＥＹ＿ＳＤ）の関係を示している。デバイスキー（ＤｅｖＫＥＹ＿ＳＤ）はそれぞれ１６列のインデックス（ＩＮＤＥＸ）とそれに対応するキー情報（ＫＥＹ）とから構成されており、メディアキーブロック（ＭＫＢ＿ＳＤ１）は１６列×５１２行程度の暗号化されたキーマトリクス群から構成されている。デバイスキー（ＤｅｖＫＥＹ＿ＳＤ）の各列のインデックスの値はメディアキーブロック（ＭＫＢ＿ＳＤ１）上の参照位置を示すものであり、各インデックスと同一列で、そのインデックスの値で指定される行位置のキー情報が参照される。例えば、第１列のインデックス値が図示のように“１”の場合には、メディアキーブロック（ＭＫＢ＿ＳＤ１）上の第１列・第１行の位置が参照される。その位置には、デバイスキー（ＤｅｖＫＥＹ＿ＳＤ）の第１列のキー（ここでは“Ａ”）によって暗号化されたメディアキーＡ［Ｋｍ］、あるいはエラーコードＡ［Ｅｃ］が格納されている。エラーコードは、該当するデバイスキーが無効であることを意味する。１６個のインデックスのいずれか一つによって、対応するキー情報（ＫＥＹ）によって暗号化されたメディアキーを取得できれば、認証が成功したことになる。この構成により、最大で512^{16}個のデバイスキーを無効化することができる。

【００３４】図２（Ｂ）はＤＶＤ－ＲＡＭメディア用のメディアキーブロック（ＭＫＢ＿ＲＡＭ）とデバイスキー（ＤｅｖＫＥＹ＿ＲＡＭ）の関係を示している。デバイスキー（ＤｅｖＫＥＹ＿ＲＡＭ）はそれぞれ１６列のインデックス（ＩＮＤＥＸ）とそれに対応するキー情報（ＫＥＹ）とから構成されており、メディアキーブロック（ＭＫＢ＿ＲＡＭ）は、１６列×２０４８行程度の暗号化されたキーマトリクス群から構成されている。これにより、メディアキーブロック（ＭＫＢ＿ＲＡＭ）においては、最大で2048^{16}個のデバイスキーを無効化することができる。

【００３５】（コンテンツの暗号化／復号化）次に、図３を参照して、記録メディアを用いて行うコンテンツの暗号化／復号化の原理について説明する。ここでは、ＳＤメモリカードを例示して説明することにする。

【００３６】＜コンテンツ記録時＞図３（Ａ）はコンテンツ記録時の処理の流れを示している。まず、ＳＤメモリカード用のメディアキーブロック（ＭＫＢ＿ＳＤ１）とＳＤメモリカード１０１に記録されているメディアキーブロック（ＭＫＢ＿ＳＤ１）とを用いた認証処理が行われ（プロセス＃１）、メディアキーＫｍが生成される。

【００３７】このメディアキーＫｍとＳＤメモリカード１０１に記録されているメディアＩＤ（Ｍｅｄｉａ　ＩＤ１）との演算処理（プロセス＃２）により、メディア固有キー（Ｋｍｕ＿ＳＤ１）が生成される。次いで、所定のタイトルキーＫｔをメディア固有キー（Ｋｍｕ＿ＳＤ１）で暗号化する処理（プロセス＃３）が実行され、これによってＫｍｕ＿ＳＤ１［Ｋｔ］が生成される。また、記録対象のコンテンツに対してはタイトルキーＫｔによって暗号化する処理が施され（プロセス＃４）、Ｋｔ［Ｃｏｎｔｅｎｔ］が生成される。そして、Ｋｍｕ＿ＳＤ１［Ｋｔ］とＫｔ［Ｃｏｎｔｅｎｔ］がＳＤメモリカード１０１に記録される。

【００３８】＜コンテンツ再生時＞図３（Ｂ）はコンテンツ再生時の処理の流れを示している。まず、ＳＤメモリカード用のメディアキーブロック（ＭＫＢ＿ＳＤ１）とＳＤメモリカード１０１に記録されているメディアキーブロック（ＭＫＢ＿ＳＤ１）とを用いた認証処理が行われ（プロセス＃５）、メディアキーＫｍが生成される。

【００３９】このメディアキーＫｍとＳＤメモリカード１０１に記録されているメディアＩＤ（Ｍｅｄｉａ　ＩＤ１）との演算処理（プロセス＃６）により、メディア固有キー（Ｋｍｕ＿ＳＤ１）が生成される。次いで、暗号化されたタイトルキーＫｍｕ＿ＳＤ１［Ｋｔ］を、メディア固有キー（Ｋｍｕ＿ＳＤ１）で復号する処理（プロセス＃７）が実行され、これによってタイトルキーＫｔが得られる。また、暗号化されたコンテンツＫｔ［Ｃｏｎｔｅｎｔ］に対しては、それをタイトルキーＫｔによって復号する処理が施され（プロセス＃８）、これによりＣｏｎｔｅｎｔが得られ、それが再生される。

【００４０】（ＤＶＤ－ＲＡＭドライバのインストール）次に、図４を参照して、ＳＤメモリカード用の最新のメディアキーブロックＭＫＢ＿ＳＤ２をＤＶＤ－ＲＡＭメディア２０１に書き込む処理について説明する。

【００４１】この書込処理は、ＤＶＤ－ＲＡＭドライバ３０３のインストール時にそのインストーラによって行われ、またインストール後はＤＶＤ－ＲＡＭドライバ３０３に付属するセットアッププログラムを起動することによって任意のタイミングで行うことができる。もちろん、書込処理を実行に当たっては、「ＤＶＤ－ＲＡＭメディアをＳＤメモリカードと同等に扱う機能を追加しますか」というメッセージがユーザに提示され、ユーザから追加する旨の応答があった場合にのみ書込処理が実行されることになる。

【００４２】なお、このインストーラ（またはセットアッププログラム）４０１はＤＶＤ－ＲＡＭドライバ３０３の一部として考えることもでき、その意味で、メディ

アキーブロックＭＫＢ＿ＳＤ２の書き込みを行うのはＤＶＤ－ＲＡＭドライバ３０３であると言うこともできる。

【００４３】（１）インストーラ（またはセットアッププログラム）４０１は、ＤＶＤ－ＲＡＭメディア用のデバイスキー（ＤｅｖＫＥＹ＿ＲＡＭ）を有している。インストーラ（またはセットアッププログラム）４０１は、デバイスキー（ＤｅｖＫＥＹ＿ＲＡＭ）とＤＶＤ－ＲＡＭメディア２０１のリードインエリアに記録されているメディアキーブロック（ＭＫＢ＿ＲＡＭ）とを用いて、ＤＶＤ－ＲＡＭメディア２０１との間の認証を行い、これによってメディア固有キー（Ｋｍｕ＿ＲＡＭ）を得る（プロセス＃１１）。この場合、まず、デバイスキー（ＤｅｖＫＥＹ＿ＲＡＭ）によってメディアキーブロック（ＭＫＢ＿ＲＡＭ）を参照することにより、メディアキーＫｍが得られ、次いで、そのメディアキーＫｍとＤＶＤ－ＲＡＭメディア２０１のリードインエリアに記録されているＤＶＤ－ＲＡＭメディア固有のメディアＩＤ（Ｍｅｄｉａ　ＩＤ２）とからメディア固有キー（Ｋｍｕ＿ＲＡＭ）が生成されることになる。

【００４４】（２）インストーラ（またはセットアッププログラム）４０１は、ＷＥＢサーバ５０１からＳＤメモリカード用の最新のメディアキーブロック（ＭＫＢ＿ＳＤ２）を取得する（プロセス＃１２）。

（３）インストーラ（またはセットアッププログラム）４０１は、メディアキーブロック（ＭＫＢ＿ＳＤ２）をＤＶＤ－ＲＡＭメディア固有のメディア固有キー（Ｋｍｕ＿ＲＡＭ）で暗号化し（Ｋｍｕ＿ＲＡＭ［ＭＫＢ＿ＳＤ２］）、それをＤＶＤ－ＲＡＭメディア２０１のユーザデータエリアに書き込む（プロセス＃１３）。

【００４５】（コンテンツの書き込み）次に、図５を参照して、ＤＶＤ－ＲＡＭメディア２０１へのコンテンツの書き込み動作を説明する。ここでは、ＳＤメモリカード１０１に記録されているコンテンツをＤＶＤ－ＲＡＭメディア２０１にコピーまたは移動する場合を想定する。

【００４６】（１）アプリケーションプログラム３０１は、デバイスキー（ＤｅｖＫＥＹ＿ＳＤ）とＳＤメモリカード１０１に記録されているメディアキーブロック（ＭＫＢ＿ＳＤ１）とを用いて、ＳＤメモリカード１０１との間の認証をＳＤドライバ３０２を介して行い、これによってメディア固有キー（Ｋｍｕ＿ＳＤ１）を得る（プロセス＃２１）。この場合、まず、デバイスキー（ＤｅｖＫＥＹ＿ＳＤ）によってメディアキーブロック（ＭＫＢ＿ＳＤ１）を参照することにより、メディアキーＫｍが得られ、次いで、そのメディアキーＫｍとＳＤメモリカード１０１に記録されているＳＤメモリカード固有のメディアＩＤ（Ｍｅｄｉａ　ＩＤ１）とからメディア固有キー（Ｋｍｕ＿ＳＤ１）が生成されることになる。

【００４７】（２）アプリケーションプログラム３０１は、ＳＤドライバ３０２を介してＳＤメモリカード１０１から暗号化されたタイトルキー（Ｋｍｕ＿ＳＤ１［Ｋｔ］）を読み出し、それをメディア固有キー（Ｋｍｕ＿ＳＤ１）で復号してＫｔを得る（プロセス＃２２）。

【００４８】（３）アプリケーションプログラム３０１は、ＤＶＤ－ＲＡＭメディア２０１との認証要求をＤＶＤ－ＲＡＭドライバ３０３に発行する。これに応答して、ＤＶＤ－ＲＡＭドライバ３０３は、デバイスキー（ＤｅｖＫＥＹ＿ＲＡＭ）とＤＶＤ－ＲＡＭメディア２０１のリードインエリアに記録されているメディアキーブロック（ＭＫＢ＿ＲＡＭ）とを用いて、ＤＶＤ－ＲＡＭメディア２０１との間の認証を行い、これによってメディア固有キー（Ｋｍｕ＿ＲＡＭ）を得る（プロセス＃２３）。この場合、まず、デバイスキー（ＤｅｖＫＥＹ＿ＲＡＭ）によってメディアキーブロック（ＭＫＢ＿ＲＡＭ）を参照することにより、メディアキーＫｍが得られ、次いで、そのメディアキーＫｍとＤＶＤ－ＲＡＭメディア２０１のメディアＩＤ（Ｍｅｄｉａ　ＩＤ２）とからメディア固有キー（Ｋｍｕ＿ＲＡＭ）が生成されることになる。

【００４９】（４）ＤＶＤ－ＲＡＭドライバ３０３は、ＤＶＤ－ＲＡＭメディア２０１に暗号化されて記録されているメディアキーブロック（Ｋｍｕ＿ＲＡＭ［ＭＫＢ＿ＳＤ２］）を読み出し、それをメディア固有キー（Ｋｍｕ＿ＲＡＭ）で復号して、ＭＫＢ＿ＳＤ２を得る（プロセス＃２４）。そして、ＭＫＢ＿ＳＤ２をアプリケーションプログラム３０１に渡す。

【００５０】（５）（６）アプリケーションプログラム３０１は、ＤＶＤ－ＲＡＭドライバ３０３からＭＫＢ＿ＳＤ２を取得すると、そのＭＫＢ＿ＳＤ２とデバイスキー（ＤｅｖＫＥＹ＿ＳＤ）とを用いて、ＤＶＤ－ＲＡＭメディア２０１との間の認証を行い、これによってメディア固有キー（Ｋｍｕ＿ＳＤ２）を得る（プロセス＃２５）。この場合、まず、デバイスキー（ＤｅｖＫＥＹ＿ＳＤ）によってメディアキーブロック（ＭＫＢ＿ＳＤ２）を参照することにより、メディアキーＫｍが得られ、次いで、そのメディアキーＫｍとＤＶＤ－ＲＡＭメディア２０１のメディアＩＤ（Ｍｅｄｉａ　ＩＤ２）とからメディア固有キー（Ｋｍｕ＿ＳＤ２）が生成されることになる。

【００５１】（７）アプリケーションプログラム３０１は、プロセス＃２２で得られたタイトルキーＫｔをメディア固有キー（Ｋｍｕ＿ＳＤ２）で暗号化し、Ｋｍｕ＿ＳＤ２［Ｋｔ］を得る。そして、そのＫｍｕ＿ＳＤ２［Ｋｔ］を、ＤＶＤ－ＲＡＭドライバ３０３を介してＤＶＤ－ＲＡＭメディア２０１に書き込む（プロセス＃２６）。

【００５２】（８）アプリケーションプログラム３０１は、暗号化されたコンテンツ（Ｋｔ［Ｃｏｎｔｅｎ

15

t]）をSDメモリカード１０１から読み込み、それをDVD－RAMドライバ３０３を介してDVD－RAMメディア２０１に書き込む。

【００５３】（コンテンツの再生）次に、図６を参照して、DVD－RAMメディア２０１に記録されているコンテンツをアプリケーションプログラム３０１が再生する場合の動作について説明する。

【００５４】（１）アプリケーションプログラム３０１は、DVD－RAMメディア２０１との認証要求をDVD－RAMドライバ３０３に発行する。これに応答して、DVD－RAMドライバ３０３は、デバイスキー（DevKEY_RAM）とDVD－RAMメディア２０１のリードインエリアに記録されているメディアキーブロック（MKB_RAM）とを用いて、DVD－RAMメディア２０１との間の認証を行い、これによってメディア固有キー（Kmu_RAM）を得る（プロセス＃３１）。この場合、まず、デバイスキー（DevKEY_RAM）によってメディアキーブロック（MKB_RAM）を参照することにより、メディアキーKmが得られ、次いで、そのメディアキーKmとDVD－RAMメディア２０１のメディアＩＤ（Media　ID2）とからメディア固有キー（Kmu_RAM）が生成されることになる。

【００５５】（２）DVD－RAMドライバ３０３は、DVD－RAMメディア２０１に暗号化されて記録されているメディアキーブロック（Kmu_RAM［MKB_SD2］）を読み出し、それをメディア固有キー（Kmu_RAM）で復号して、MKB_SD２を得る（プロセス＃３２）。そして、MKB_SD２をアプリケーションプログラム３０１に渡す。

【００５６】（３）（４）アプリケーションプログラム３０１は、DVD－RAMドライバ３０３からMKB_SD２を取得すると、そのMKB_SD２とデバイスキー（DevKEY_SD）とを用いて、DVD－RAMメディア２０１との間の認証を行い、これによってメディア固有キー（Kmu_SD２）を得る（プロセス＃３３）。この場合、まず、デバイスキー（DevKEY_SD）によってメディアキーブロック（MKB_SD２）を参照することにより、メディアキーKmが得られ、次いで、そのメディアキーKmとDVD－RAMメディア２０１のメディアＩＤ（Media　ID2）とからメディア固有キー（Kmu_SD２）が生成されることになる。

【００５７】（７）アプリケーションプログラム３０１は、DVD－RAMドライバ３０３を介してDVD－RAMメディア２０１から暗号化されたタイトルキー（Kmu_SD２［Kt］）を読み出し、それをメディア固有キー（Kmu_SD２）で復号してKtを得る（プロセス＃３４）。

【００５８】（８）アプリケーションプログラム３０１は、DVD－RAMドライバ３０３を介してDVD－RAMメディア２０１から暗号化されたコンテンツ（Kt［Content］）を読み出し、それをKtで復号して再生する（プロセス＃３５）。

16

【００５９】以上のように、本実施形態においては、DVD－RAMメディア／ドライブ用の制御プログラムであるDVD－RAMドライバ３０３によってSDメモリカード用のメディアキーブロックMKB_SDをDVD－RAMメディア２０１上に記録し、その記録したメディアキーブロックMKB_SDを用いてDVD－RAMメディア２０１との認証をアプリケーションプログラム３０１に実行させることにより、SDメモリカード用のデバイスキーDev　KEY_SDで、DVD－RAMメディアも扱うことが可能となる。よって、著作権保護機能に対応した正当な記録メディアであればその種別を意識することなく、それら記録メディアを透過的に扱うことが可能となる。

【００６０】特に、SDメモリカード用のメディアキーブロックMKB_SDを、MKB_RAMとの認証によって得たKmu_RAMによって暗号化した状態でDVD－RAMメディア２０１に書き込むことにより、結果的にメディアキーブロックMKB_SDとMKB_RAMとが関連づけられた形となるので、MKB_SDの秘匿化を図ることが可能となる。

【００６１】なお、本実施形態では、最新のメディアキーブロックMKB_SD２を取得してDVD－RAMメディアに記録したが、これは排除すべきデバイスキーの増加に対応させるためである。したがって、SDメモリカードに記録されているMKB_SDが最新のもの、あるいは比較的新しいものであれば、それをDVD－RAMメディアに記録するようにしても良い。

【００６２】また、コンテンツの暗号化鍵であるタイトルキーをメディア固有キーを用いて暗号化するようにしてが、メディア固有キーをタイトルキーとして使用し、コンテンツ自体をメディア固有キーを用いて暗号化するようにしてもよい。

【００６３】また、DVD－RAMメディアとSDメモリカードに限らず、他の各種記録メディアにも同様の方法を適用することができる。

【００６４】さらに、本実施形態は、PCに限らず、セットトップボックス、ゲーム機、オーディオ／ビデオプレイヤーなど、マイクロプロセッサを搭載したあらゆるデータ処理装置（コンピュータ応用機器）に適用することができる。

【００６５】また、本実施形態で説明したコンテンツ管理方法の手順を記述したコンピュータプログラムを記録媒体を通じてコンピュータまたはコンピュータ応用機器に導入することにより、本実施形態と同様の効果を容易に得ることができる。

【００６６】

【発明の効果】以上説明したように、本発明によれば、ある特定のメディア種別に対応したデバイス識別情報によって他のメディア種別の記録メディアを扱えるようになり、著作権保護機能に対応した正当な記録メディアであればその種別を意識することなく、それら記録メディアを透過的に扱うことが可能となる。よって、拡張性、互換性に優れたコンテンツ管理を実現できる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るコンテンツ処理システムの基本構成を示すブロック図。

【図２】同実施形態のシステムで使用されるメディアキーブロックとデバイスキーとの関係を説明するための図。

【図３】同実施形態のシステムで使用されるコンテンツの暗号化／復号化の原理を説明するための図。

＊【図４】同実施形態のシステムで行われるメディアキーブロックの書き込み処理の手順を説明するための図。

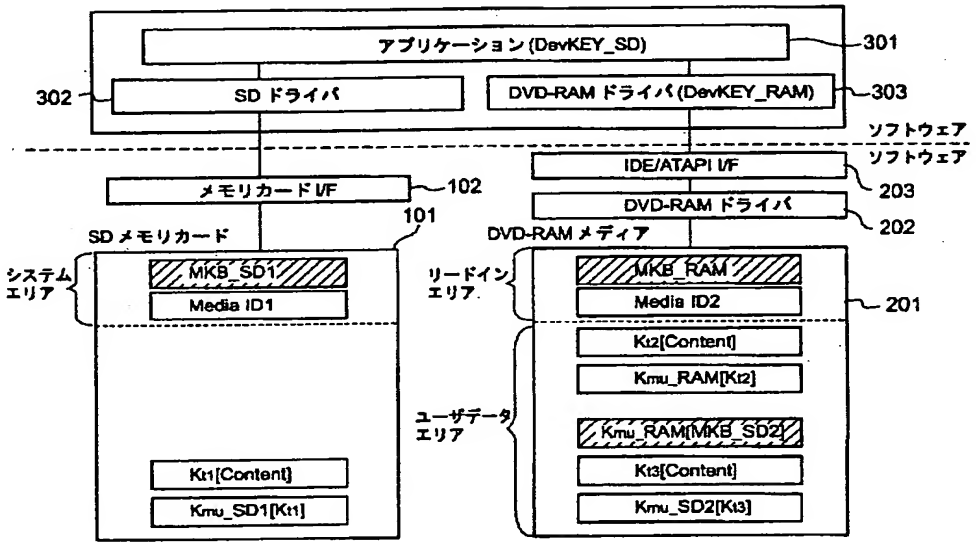
【図５】同実施形態のシステムで行われるコンテンツ書き込み処理の手順を説明するための図。

【図６】同実施形態のシステムで行われるコンテンツ再生処理の手順を説明するための図。

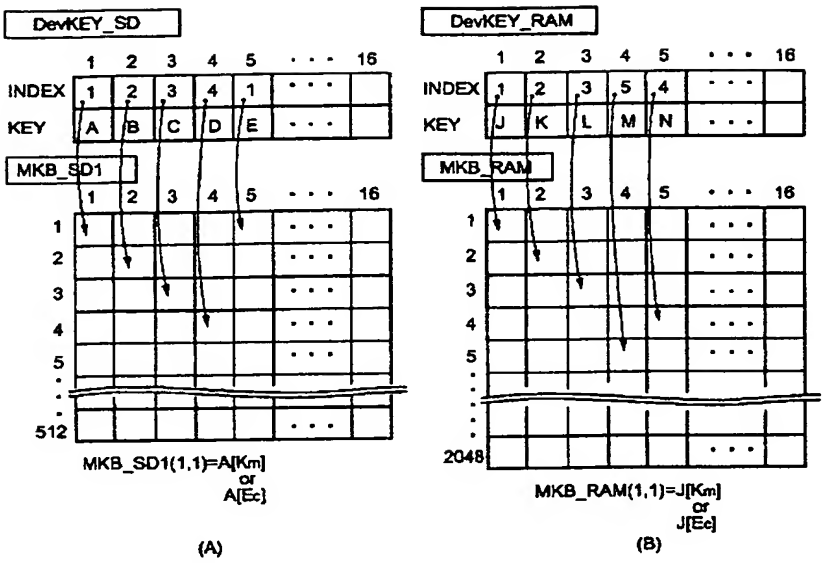
【符号の説明】

１０１…ＳＤメモリカード
１０２…メモリカードインターフェース
２０１…ＤＶＤ－ＲＡＭメディア
２０２…ＤＶＤ－ＲＡＭドライブ
２０３…ＩＤＥ／ＡＴＡＰＩインターフェース
３０１…アプリケーションプログラム
３０２…ＳＤドライバ
３０３…ＤＶＤ－ＲＡＭドライバ

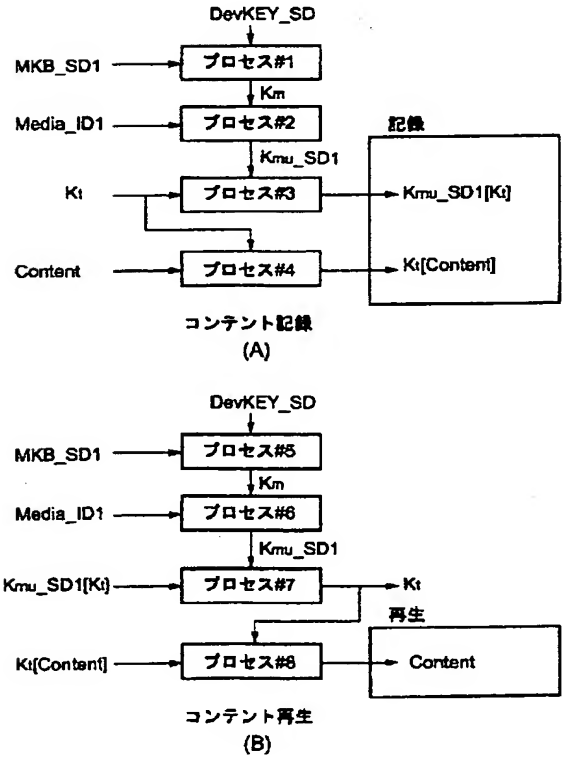
【図１】



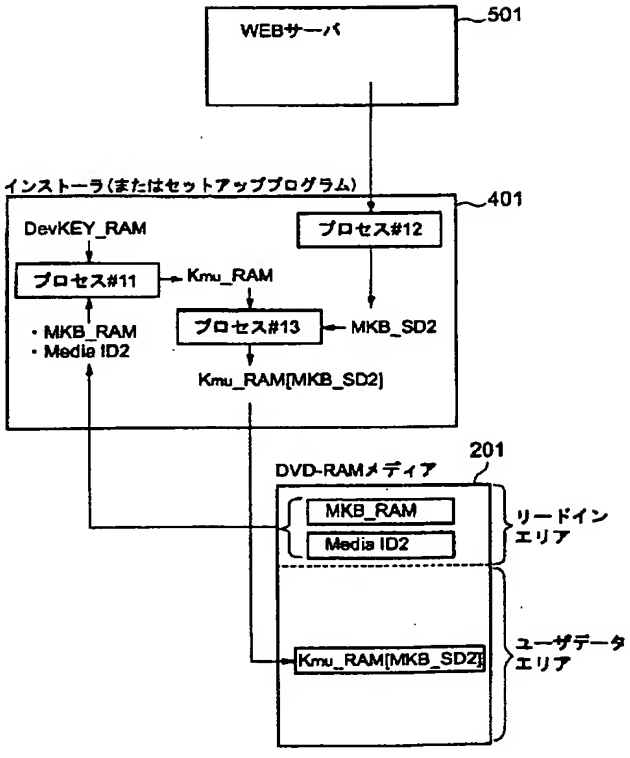
【図２】


DevKEY_SD
INDEX
KEY
MKB_SD1
MKB_SD1(1,1)=A[Km] or A[Ec]
(A)
DevKEY_RAM
INDEX
KEY
MKB_RAM
MKB_RAM(1,1)=J[Km] or J[Ec]
(B)

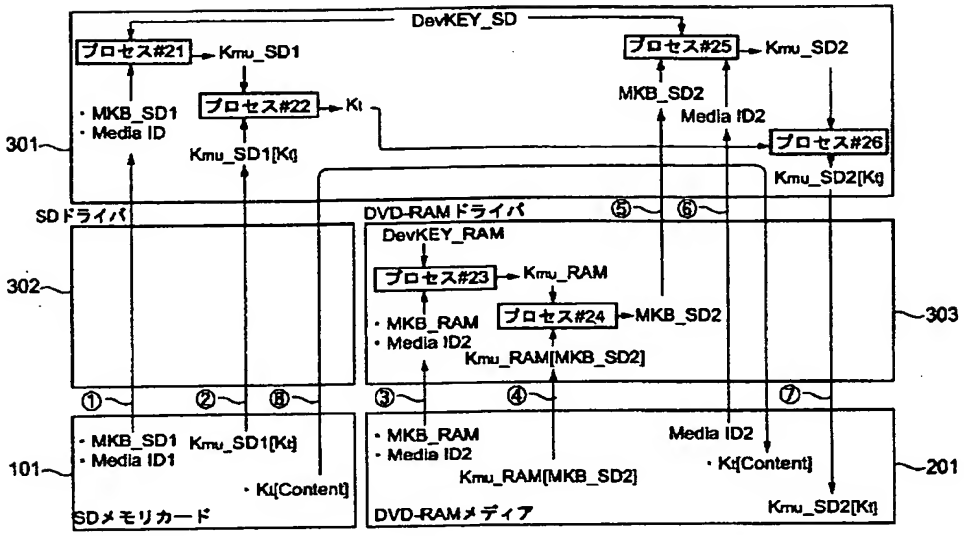
【図３】


DevKEY_SD
MKB_SD1
プロセス#1
Km
Media_ID1
プロセス#2
Kmu_SD1
Kt
プロセス#3
Kmu_SD1[Kt]
Content
プロセス#4
Kt[Content]
記録
コンテント記録
(A)
DevKEY_SD
MKB_SD1
プロセス#5
Km
Media_ID1
プロセス#6
Kmu_SD1
Kmu_SD1[Kt]
プロセス#7
Kt
再生
Kt[Content]
プロセス#8
Content
コンテント再生
(B)

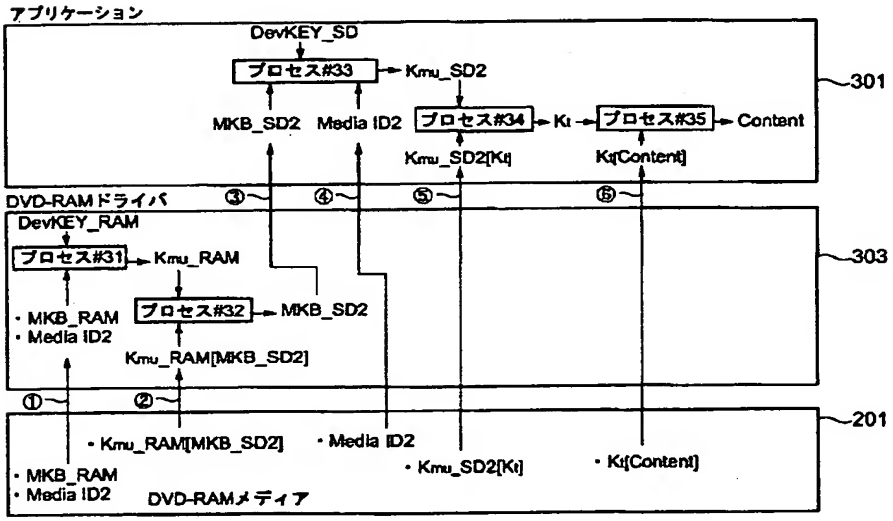
【図４】


WEBサーバ
501
インストーラ(またはセットアッププログラム)
401
DevKEY_RAM
プロセス#12
プロセス#11
Kmu_RAM
・MKB_RAM
・Media ID2
プロセス#13
MKB_SD2
Kmu_RAM[MKB_SD2]
201
DVD-RAMメディア
MKB_RAM
Media ID2
リードイン エリア
Kmu_RAM[MKB_SD2]
ユーザデータ エリア

【図５】


DevKEY_SD
プロセス#21
Kmu_SD1
プロセス#22
Kt
プロセス#25
Kmu_SD2
MKB_SD2
Media ID2
プロセス#26
Kmu_SD2[Kt]
・MKB_SD1
・Media ID
Kmu_SD1[Kt]
301
SDドライバ
DVD-RAMドライバ
⑤
⑥
DevKEY_RAM
プロセス#23
Kmu_RAM
302
・MKB_RAM
・Media ID2
プロセス#24
MKB_SD2
303
Kmu_RAM[MKB_SD2]
①
②
⑧
③
④
⑦
・MKB_SD1
・Media ID1
Kmu_SD1[Kt]
・MKB_RAM
・Media ID2
Media ID2
・Kt[Content]
101
・Kt[Content]
Kmu_RAM[MKB_SD2]
201
SDメモリカード
DVD-RAMメディア
Kmu_SD2[Kt]

【図６】


アプリケーション
DevKEY_SD
プロセス#33
Kmu_SD2
301
MKB_SD2
Media ID2
プロセス#34
Kt
プロセス#35
Content
Kmu_SD2[Kt]
Kt[Content]
DVD-RAMドライバ
③
④
⑤
⑥
DevKEY_RAM
プロセス#31
Kmu_RAM
303
・MKB_RAM
・Media ID2
プロセス#32
MKB_SD2
Kmu_RAM[MKB_SD2]
①
②
201
・Kmu_RAM[MKB_SD2]
・Media ID2
・Kmu_SD2[Kt]
・Kt[Content]
・MKB_RAM
・Media ID2
DVD-RAMメディア